ABSTRACT OF THE DISCLOSURE

A general finite-field multiplier and the method of the same are disclosed for the operation of the finite-field multipliers of various specifications. In the multiplier, AND gates and XOR gates are used as primary components, and the inputs include two elements A and B to be multiplied and the coefficients of a variable polynomial p(x). This multiplier can be applied to the finite-field elements of different bit number. After all the coefficients of the A, B and p(x) are input, the values of a desired C can be obtained rapidly. Since the output values are parallel output, the application is very convenient. Furthermore, the multiplier can be used in the RS chip for different specifications.